法が私たちの権利に背くとき

——米国の監視社会とジェンダーを事例に——

JCA-NET セミナー　2023/8/26

小倉利丸
toshi@jca.apc.org
https://www.jca.apc.org

2023/8/26 11:30 改訂

マイナ保険証とないがしろにされる医療情報のプライバシー

マイナンバー / カードと保険証の一体化をめぐる最大の問題は、医療情報を第三者にアクセスさせるリスクが限りなく広がりをみせるに違いない、ということだ。

医療情報は、医療従事者と私だけが知ることができればいい事柄だ。だから第三者が医療情報にアクセスすること自体を禁じるべきでもある。実際には医療保険制度によって、この厳格なプライバシーは保護することができない。マイナ保険証は、マイナンバーを介して将来的には、全国どこでも、そしてたぶん、様々な行政や民間企業もまた、医療情報の共有を可能にしようとする思惑をもったものだ。杜撰なシステムの設計によって、この政府の目論見は挫折しているが、マイナ保険証の問題は、医療行為のプライバシーが根底から揺らぎかねない問題でもある、ということを忘れてはならないと思う。

今回取り上げる米国における中絶の違法化 (犯罪化) は、医療とプライバシーの権利を考える上で、非常に重要な問題を提起していると思う。しかも、医療プライバシーの問題は、医療だけの問題ではなく、人々の日常生活全体の行動がデータ化されてプロファイルされる現代の監視社会全体の仕組みと密接に関わっている。米国が直面しているリプロダクティブライツの深刻な危機にあって、人々がどのような闘いによって、この危機を打ち返そうとしているのかもまた、私たちにとって学ぶべき点が多いと思う。

ロー対ウェイド判決

2022年6月 連邦最高裁判所はロー対ウェイド判決の立場を否定し、人工妊娠中絶に対する憲法上の保護を取り消した。

その後1年の動き

- 15の州で人工妊娠中絶禁止が制定され半数の州で試行
- 2023年には全米で142の法案が提出され
- 20の州ではすでに青少年に対するジェンダー・アファメーション・ケアが禁止
- 7つの州ではすべての年齢の人々に対するジェンダー・アファメーション・ケアが禁止

ジェンダー・アファメーション・ケア：生物学的な性に規定されることなく、ジェンダーの自認に基いて生きるために必要な医療ケア

トリガー法 v.s. セーフヘブン法

判決が出された直後から一気に中絶禁止が広がりをみせた理由は、「トリガー法」(「トリガー禁止」ともいう)という法制度があるからだ。

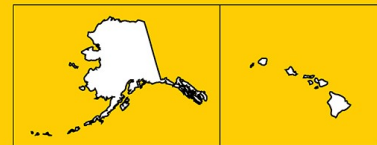
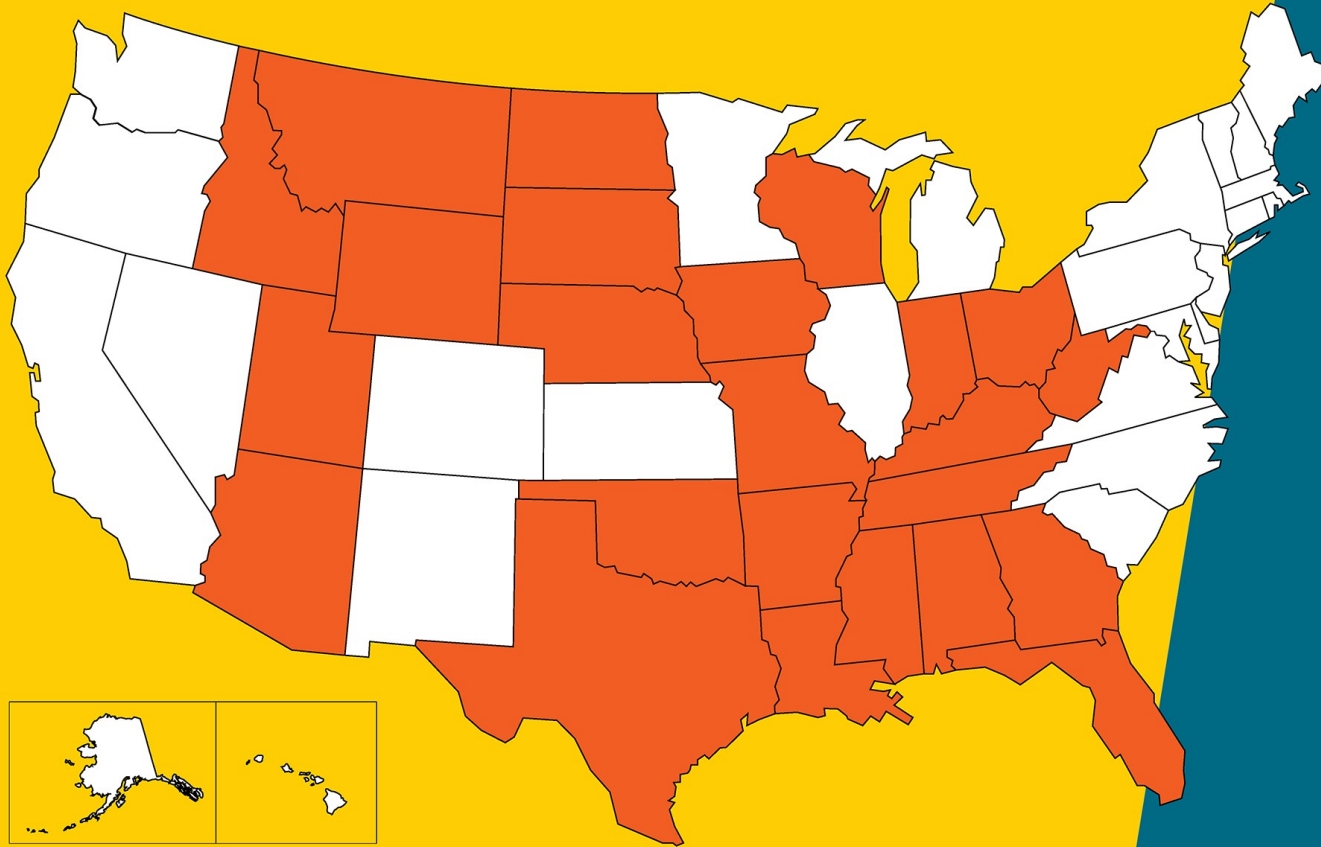
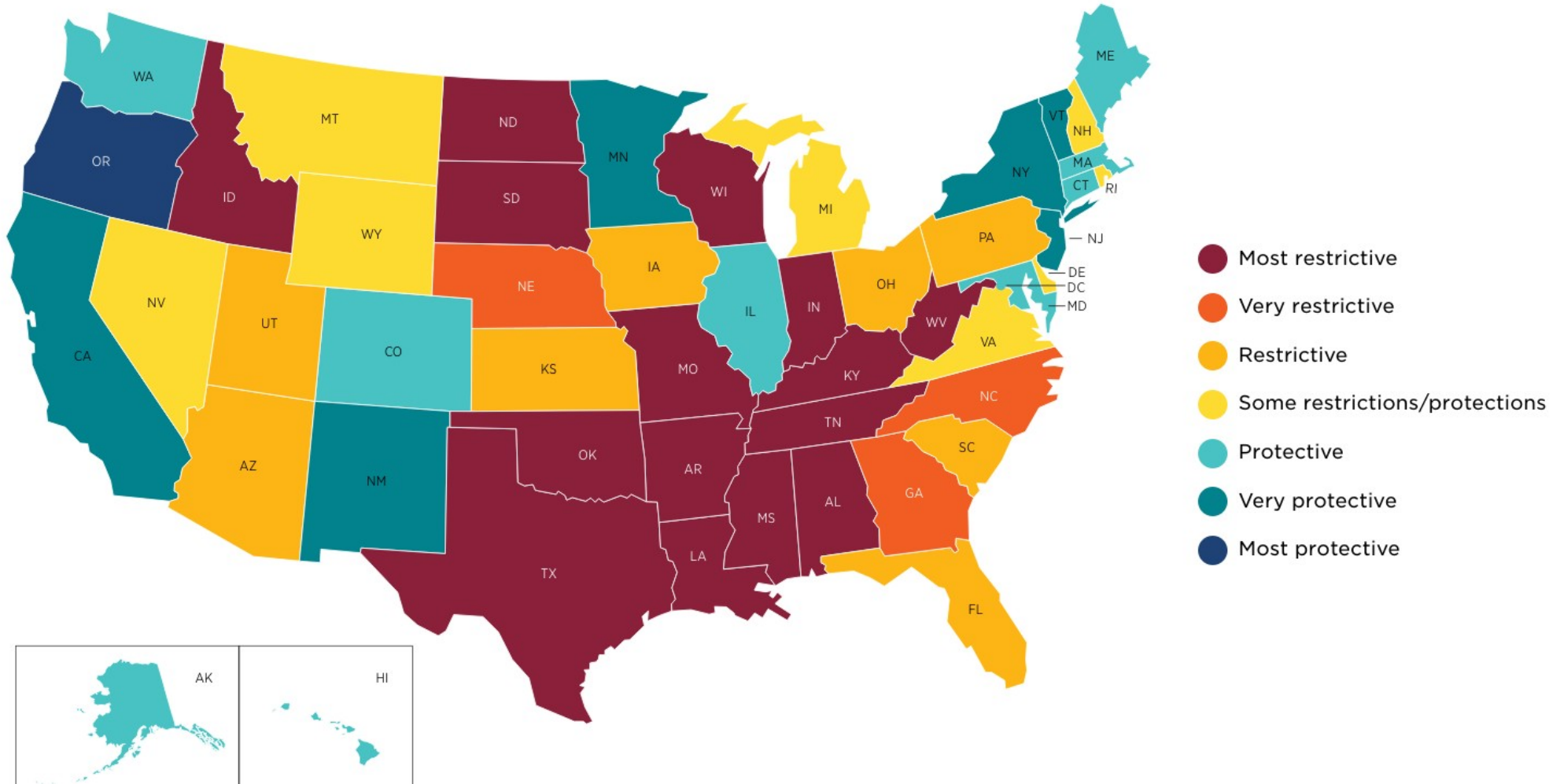
- ロー判決が覆されて中絶禁止が合憲とされることを見越して、中絶反対派が、中絶が禁止されたり、大幅に制限される可能性のある最高裁判決に先んじるために考案したもの。
- 中絶禁止に踏み切るとみられる26の州のうち13州は、ローが適用されなくなった場合、自動的に、あるいは迅速な州の行動によって「発動」され、発効するように設計された法律を制定。

つまり

- 最高裁判決がなければ中絶禁止を法制化する共和党優位の州の存在
- 最高裁判決で中絶が合憲とされた時代でも、根強い反中絶運動が継続
- トランプ政権下での、最高裁判事が保守派優位になったことで、トリガー法が加速化

参考：「(guttmacher) 13の州で妊娠中絶のトリガー禁止 -- ローが覆されるとどうなるか」https://www.guttmacher.org/article/2022/06/13-states-have-abortion-trigger-bans-heres-what-happens-when-roe-overturned
仮訳：https://cryptpad.fr/pad/#/2/pad/view/DVfP6jTpUmMXbw+vrKtXWCEX8i3rgtBfWHb1iUncZK8/

Six months post-*Roe v. Wade*, 24 US states have banned abortion or are likely to do so
guttmacher.org

https://states.guttmacher.org/policies/

トリガー法 v.s. セーフヘブン法

中絶禁止州では、中絶が可能な州に越境して中絶することを違法とする州法の制定が進む

2023 年 4 月、アイダホ州の議員たちは、特定の中絶手術を受けるために近隣の州へ行くことを禁止。他の禁止州もこれにならう傾向がある

参考：「(guttmacher) 13 の州で妊娠中絶のトリガー禁止 -- ローが覆されるとどうなるか」https://www.guttmacher.org/article/2022/06/13-states-have-abortion-trigger-bans-heres-what-happens-when-roe-overturned
仮訳：https://cryptpad.fr/pad/#/2/pad/view/DVfP6jTpUmMXbw+vrKtXWCEX8i3rgtBfWHb1iUncZK8/

トリガー法 v.s. セーフヘブン法

中絶合法の州による「セーフヘブン法」

少なくとも16の州とワシントンD.C.は、州レベルで中絶の権利を守り続ける

カリフォルニア、コネチカット、デラウェア、ハワイ、メリーランド、ニュージャージー、ニューヨーク、オレゴン、ワシントンは、州外から中絶治療を受けに来るかもしれない人々の需要の増加に対応するために、中絶保護を強化

- 州議会 中絶クリニックにより多くの資金を振り向ける
- 健康保険プランに処置をカバーすることを義務づける
- 中絶を提供することを許される医療専門家の種類を拡大

参考 「妊娠中絶のセーフヘイブン州ができること」 https://time.com/6191581/abortion-safe-haven-states/
仮訳：https://cryptpad.fr/pad/#/2/pad/view/1+gOGNspfCRMcX5f-7xxi5nqclo3rK2OiC4sjkFfNnU/

ターゲットにされる越境「旅行者」たち

医療を求める人々の旅行への医療犯罪を起訴する検察によるデジタル監視

- 自家用車による移動の監視
- タクシー、ライドシェアの監視
- バス、地下鉄の監視
- 飛行機の監視

生殖医療やジェンダーを肯定する医療クリニックに旅行したことを暴露するために移動データを使用することができる。

米国で匿名で旅行し、旅行のデジタル痕跡を残さないようにすることはほぼ不可能だ。

参考：「S.T.O.P. レポート、中絶や性別適合ケア旅行に対する監視の脅威を詳述する」https://www.stopspying.org/latest-news/2023/7/18/stop-report-details-surveillance-threats-to-abortion-gender-affirming-care-travel （仮訳）https://cryptpad.fr/pad/#/2/pad/view/xqoqn-FUdD4kFjqTDwcRibf4A+7gNLApVOEKh2izY2I/

	交通機関と宿泊 Transport or accommodation	Risk of confirming identity to law enforcement 本人特定のリスク	Risk of confirming destination to law enforcement 目的地特定のリスク	プロファイリングのリスク Profiling risk
Last mile travel 中絶医療施設までの最後の旅程	Private vehicle 自家用車	Very high	Very high	Very high
	Rideshare vehicle (e.g., Uber) ライドシェア	Very high	Very high	Very high
	Taxi	High	High	Varies
	Municipal buses and subways バス地下鉄	Low	Very low	Very low
	Scooter and Bikeshare	Very high	Very high	Very high
Long distance travel 長距離旅行	Airplane	Very high	Low	Varies
	Long-haul bus 長距離バス	High	Low	Varies
	Amtrak 長距離列車	High	Low	Varies
Accommodations 宿泊	Hotels, motels	High	Moderate, with exceptions	Varies
	Short-term rentals	Low	Low	Very safe
	Private homes	Very low	Very low	Very safe (except public housing)

自家用車のリスク

自動車の監視

少なくとも1990年代から、中絶反対派の過激派は生殖医療クリニックに駐車している車のナンバープレートデータを収集し、それらの車の所有者を特定し、この情報を使ってクリニックの訪問者やスタッフに脅迫電話や郵便で嫌がらせ

自動ナンバープレート読み取り機（「ALPR」）

- 米国の道路や高速道路を網羅し膨大なデータを収集
- 車両、同乗者も撮影
- 光学式文字認識を使ってナンバープレート番号を抽出
- ナンバープレート番号は、カメラの位置や日時情報、時には運転手や同乗者の写真と共に保存
- ALPRの提供企業が保有し、法執行機関とも共有可能

ALPRがなくても、州外のナンバープレートは、州をまたいで中絶を行う人の目立ちやすい識別子になる

自家用車のリスク

自動車の監視 ALPRのデータのほかにも

- 駐車場に設置されたナンバープレート・リーダー
- 診療所やその近くで収集した街頭カメラの映像
  - 中絶医療を犯罪として取り締まる州のナンバープレートの車をスキャン
  - 診療所付近の街頭カメラで診療所を訪れる人の顔を撮影し、顔認識ツールを使ってスキャン

ALPRとこれらのデータを総合することによって、医療の利用者のプロファイリングが可能に。

- インフォテインメント・インターフェイス

ドライバーの携帯の機能と車の情報を統合

→ 携帯内にあれば保護されるプライバシー情報が外部のデバイスに転送されると、この保護が外される。

→ データは多くの場合無期限に保存され、自動車メーカー、レンタル会社、情報通信プロバイダー、アプリ会社、法執行機関などとも共有

自家用車以外の自動車のリスク

自家用車以外の場合

- ライドシェア：サービス提供会社は、アカウント所有者の名前、電子メールアドレス、電話番号、支払い情報、目的地データなど、個人を特定できるライダーデータを収集
- ニューヨーク市のタクシー・リムジン委員会 目的地データを含むすべてのタクシー乗車のデータベースを管理
- 公共交通のバス、地下鉄など 最終目的地がどこなのか判断。
- ニューヨーク 携帯電話やクレジットカードで運賃を支払うことを推奨。

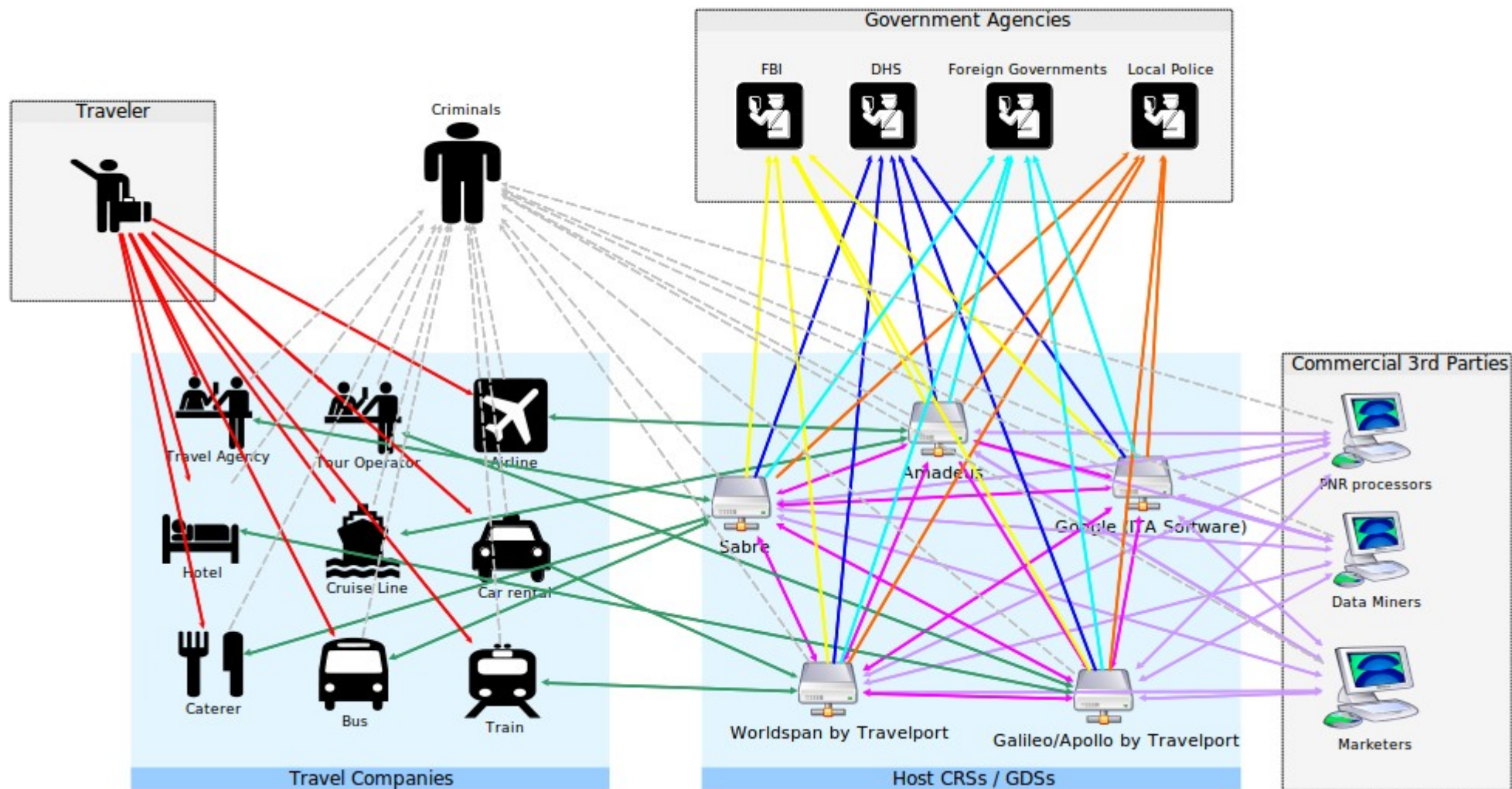
これらのデータと利用者個人の身元と経路が紐付けられ、街頭カメラの映像と組み合わせれば、目的地にいる人物を特定することができる。

飛行機のリスク

飛行機　最終目的地は不明だが、搭乗そのものは厳しく監視される。

航空券を予約

- 航空会社は搭乗者の膨大な情報を含む乗客名記録（ PNR ）を作成
- PNR データには通常、乗客の名前、電話番号、住所、性別、クレジットカード情報、 IP アドレス、さらにはエクスペディアのようなサードパーティサイトを通じて予約された場合はホテルや車の予約情報まで含まれている

https://cryptpad.fr/pad/#/3/pad/edit/4616159e7004b489dffbd9597f165765/

警察のプロファイリングの歴史

警察のプロファイリングの歴史は、社会から疎外されたコミュニティのメンバーが主なターゲットになってきた。

- 1975年までは、中南米系と思われ、国境付近を旅行していることが交通取り締まりの口実となっていた。
- 以後、移民税関捜査局は旅行データをハイテク化し、2020年には、何百万台ものスマートフォンから位置情報を購入し使用することで、旅行に基づいて非正規滞在者をプロファイリング。
- 麻薬取締局（「DEA」）は、要警戒都市から飛行機で移動する、航空券を現金で支払う、手荷物を預けない、といった渡航の特徴にフラグを立てる。
- DEAの捜査官は、直感に基づいて旅行者を止める行為を行なっている。（司法省が人種プロファイリングとしている行為）

警察のプロファイリングの歴史

- 9.11以降、イスラム系アメリカ人の渡航データもまた、国家安全保障上の脅威とされる彼らをプロファイリングするために利用。
- イスラム系アメリカ人やイスラム系と思われる人々は、渡航の際、余分なセキュリティチェック、空港での検査、渡航とは関係のない広範な質問など、人間性を奪うような監視の対象となってきた。
- イスラム教徒が多数派を占める国への渡航歴は、プロファイリングの口実となっている。
- 旅行者が片道航空券を購入したり、現金で支払ったり、変わった旅程を組んだり、フラグの立てられている目的地から飛行機を利用したりすると、さらに厳しく監視される。

歴史を踏まえて、現状をみると

禁止措置に対抗して、医療保護区を設ける州法が旅行者を助けている。

医療を求める人を捜査や訴追から効果的に守るためには、禁止州の制度が匿名での渡航や現金での支払いを制限または禁止したり、捜査機関や反中絶団体が医療を求める人の個人データ（渡航データ、医療データ、スマートフォンのデータ、支払いデータ）を収集したり暴露したり共有するなどの行為を阻止することが必要。

- 法制度による対抗
- 技術的対抗

深刻な現状

ロー対ウェイド事件、家族計画連盟対ケイシー事件、そして中絶に関する連邦憲法上の権利を破棄は、<u>1973年以前への先祖返りではなく、時代遅れの中絶法が最先端のテクノロジーで施行される、はるかに暗い未来</u>になる。

- 警察、検察、そして民間の中絶反対派は、アメリカの既存の監視インフラを武器に、妊娠中の人々を標的にし、法廷において彼らの健康データを悪用してきた。
- 中絶反対派は、妊娠中の人々や中絶提供者を監視し、彼らの生殖の自由を脅かそうとする。
- 病院は疑惑もないなかで薬物検査で妊娠中の患者を追跡する。
- 検索履歴、オンラインショッピング、メッセージなど、妊娠中の人々のオンライン生活のほぼすべての側面がすでに標的とされており、携帯電話の位置データは物理的空間における彼らの動きを追跡するために使用される。

参考：「(S.T.O.P)妊娠パノプティコン——ポスト・ロー判決の中絶監視」https://www.stopspying.org/pregnancy-panopticon（仮訳）
https://cryptpad.fr/pad/#/2/pad/view/v0L8bm7BEhPBmcBqzU9XwNkpx0IWAkovJEkvkII3atk/

将来はどうなるのか？

中絶反対派がやってきたこと

リプロダクティブ・ライツ（性と生殖に関する権利）の行使を妨げるために、監視戦術を使用してきた。

- 中絶を求める人々や医療スタッフを撮影し、公に暴露
- 患者のソーシャルネットワークをマッピング
- その家族に接触し、家族への強制や暴力さえも引き起こす
- 診療所に入る人々のナンバープレートを追跡
- 生殖医療提供者の名前、住所、電話番号、および写真を、各医師に"労働"、"負傷"、"死亡"のラベルを貼って掲載したウェブサイトまで作成

将来はどうなるのか？

中絶が権利とされていた状況であっても、医師は監視の対象であるだけでなく、医師は妊娠中の人々への監視者でもある。医療スタッフは事実上、令状も同意もなしに妊娠中の患者を薬物検査し、結果を警察に報告する犯罪捜査官として動員されている。

今後は、このような医療監視は、ポスト・ローの世界ではさらに拡大し、アメリカの医師や看護師を警察官に仕立て上げ、医師、看護師、患者の間の信頼関係を破壊する。

将来はどうなるのか？

ニューヨークのような権利保護州に住む幸運な人々でさえ、妊娠中の人々にとっては生活のあらゆる面で試練が増える。たとえば、

- 中絶の形跡がないか調べられる。
- 州当局は中絶法に基づいて告発するため、私たちの生活の最も親密な側面を覗き見るためにテクノロジーを使用→これまでの取り締まりの監視ツールに目を向けるようになっている。
- 中絶医療の縮小が起きている。これが、妊娠中の人々に致命的な結果をもたらしており、多くの人々が危険な民間療法に頼っている。
- 中絶で不当に起訴されることや、医師に伝えた情報が法廷で不利に使用されることを恐れ、流産の治療を見送らざるを得なくなり、筆舌に尽くしがたい苦しみを味わう。

将来はどうなるのか？

私たちにできることはたくさんあり、すぐに行動を起こさなければならない。

- あなたの権利を守る州は、妊娠中の人々に向けられるであろう政府の監視権限を抑制し、ジオフェンス令状や警察のデータ購入のような乱用的な手段を禁止しなければならない。
- 中絶医療提供者と擁護者は、デジタルインフラを強化し、オンラインで助けを求める妊娠中の人々のプライバシーを確保しなければならない。
- Apple、Facebook、Google のような技術大手は、暗号化とプライバシー保護を劇的に改善し、警察の大量監視を当たり前にするようなことを終わらせなければならない。

反監視の保護措置は、ドッブズで予想される破壊的な判決に直面して、中絶支持者が取ることのできる最もインパクトのある措置である。プロチョイスのリーダーたちは、9.11 以降の世界における警察の監視の役割に根本的に異議を唱えなければならないだろうが、それが意味のあるリプロダクティブ・ライツを保持するための条件である。

将来はどうなるのか？

この傾向は、アメリカ生活におけるデジタルプラットフォームが生活全体を覆うようになり、対面での中絶サービスへのアクセスが減少することによって加速している。

- 多くの中絶反対派議員の圧力で州内の中絶医療提供者の数が減少。
- 中絶薬の利用。中絶を求める人の多くは、中絶医療にアクセスするためにますますインターネットに依存するようになっている。

ネット監視：検索エンジン

- インターネットの検索エンジンは、妊娠中の人々を追跡するための特に強力なツールである。警察は妊娠している人のデバイスから検索履歴を取得できるだけでなく、検索エンジンから直接記録を取得することもでき、時には令状さえ必要ないこともある。
- 米国では、検索エンジンでの検索履歴を取得するには、国家安全保障に関するばあいは、外国情報監視裁判所（全米の連邦裁判官で構成される秘密裁判所）の令状でよい。
- 司法省が、人々の閲覧履歴や検索クエリに関するデータを入手するために、215条として知られる愛国者法の条項をどれくらいの頻度で使用しているかは明らかではない。Google、Microsoft、Mozillaなどのハイテク企業は、受け取った国家安全保障上の要請について詳細な情報を提供することを法的に禁じられている。

ネット監視：販売データ

販売データの監視

- 電子決済記録や小売店の販売データも、中絶監視の有力な情報源である。多数の中絶希望者がオンラインで中絶薬を購入することができるが、特に最も効果的な薬がいまだに処方箋によってのみ投与される場合には、匿名で処方箋を取得する方法はない
- 法執行機関は、人々が中絶誘発薬を売買したことを証明するため、あるいはそもそも妊娠していたことを証明するために、ショッピング記録を召喚することができる。購入者がクレジットカードやオンラインアカウント、あるいは店頭のポイントカードで支払う場合、日常的に購入する薬、妊娠検査薬、妊婦用ビタミン剤、生理用品は状況証拠となりうる。

ネット監視：メールと位置情報

テキストメッセージや電子メールのような暗号化されていない形式への監視

- 警察は、電子メール、ソーシャルメディア上のメッセージ、ビデオゲームプラットフォームからの通信、その他無数の形態の電子メッセージを使用して、妊娠中の人々を追跡し、告発することができる

ジオフェンス令状

- 警察が令状を取得する場合、「ジオフェンス令状」のような目新しい裁判所命令を使用することが多く、これはGoogleや 他の企業に対し、指定された時間と場所にいるすべてのユーザー（１つの部屋であれ、事実上町全体であれ）の情報を提出するよう求めるもの
- 反対派はすでに同じジオフェンシングテクノロジーを使用して他社のデータにアクセスし[23]、中絶クリニックを訪れる人々をターゲットにしてメッセージを送っている

ネット監視：囮捜査

- 偽の警察のソーシャルメディア・アカウント

警察官はインターネット上の属性管理システムinternet attribution management systemを通じて大量の偽アカウントを管理することができ、一般の人々に警察官を「友人」として受け入れてもらうことで、警察は裁判所の命令なしに個人情報にアクセスすることができる。

警察官が偽の生殖医療提供者のアカウントを通じて妊娠中の人々を特定し、中絶を求める人々を騙して身元を特定することができるようになる。

- 連邦・州・州間のデータ共有協定により、地元警察は全国の連邦・州・地方のパートナーと情報を共有する。
- 情報共有協定は、ニューヨークの住民と、同州に渡航する州外の中絶希望者の両方を監視することを促進するだろう。その結果、各州は、情報共有協定、情報融合センター、省庁間タスクフォース、連邦および州外の法執行機関とのその他のパートナーシップから脱退することで、管轄区域内の妊娠中の人々に対する監視の脅威を劇的に軽減することができる。

ネット監視：ハイテク産業 (Google)

対抗手段の提案？

国内最大手のハイテク企業の多くは、妊娠中の従業員への支援をいち早く表明

しかし、自社のデータが中絶希望者の不利になるような使われ方をしていることに言及している企業はほとんどない。

Googleが情報の保管をやめれば、ジオフェンス令状やキーワード令状、その他の検索監視の脅威をほとんどなくすことができる。

ジオロケーションデータを収集しないか、あるいはジオロケーション令状の要求に応じられるような方法で保存しないことで、多くの企業はすでに事実上ジオフェンス令状から免れている。このようなプライバシー保護は、Googleの中核事業に影響を与えることは間違いないが、そうしたビジネスを断念するによって、これらの変更は、同社が本当にリプロダクティブ・アクセスをサポートしているかどうかを測る最も意味のある指標となる。

ネット監視：：ハイテク産業 (Meta)

Meta（ Facebook の親会社 ）

暗号化されたサービスにおいて重要な設計上の選択に直面している。現在、両社は暗号化保護を大々的に宣伝しているが、実際には法執行機関の監視を容易にする妥協を行っている。近年、 Meta は WhatsApp メッセージング・プラットフォームの機能として「エンドツーエンド」暗号化を大々的に宣伝している。しかし、 Meta は WhatsApp ユーザーから、人々がいつ誰と通信したかの詳細を含む大量のデータを収集し続けている。このデータは、警察が保健医療提供者や他のサービスと通信している人々を見つけるために簡単に使用することができる。さらに懸念は、 WhatsApp にはコンテンツモデレーションツールがあり、暗号化を回避してメッセージの内容を読むことができる。

同社は Facebook メッセンジャーで限定的な暗号化保護を提供したが、ユーザーがオプトインするための面倒なプロセスを経た場合に限られる。 Meta がすべてのプラットフォームで真のエンドツーエンドの暗号化とデータ最小化の実践を実施しない限り、このプラットフォームはまとめて、警察が中絶希望者を特定する主要な方法のひとつになるだろう。

ネット監視：：ハイテク産業 (Apple)

アップル社も、暗号化対策を強化か、自社のデバイスを取り締まりツールにするか、決断を迫られる

- Appleはしばしば自社製品のプライバシーを宣伝しているが、同社のクラウドサービスは裁判所命令に対して非常に脆弱なままである。
- AppleはiCloud上のすべてのユーザーデータへのアクセス権を保持しているため、同サービスに保存されたバックアップも警察がアクセスできる可能性がある。
- AppleはiMessageサービスから暗号化された通信のコピーを保存するようユーザーに奨励しており、同様に警察がアクセスできる可能性がある。
- ユーザーは、iMessageの会話は他の誰からも、アップル社からも保護されていると言われているが、ユーザーがアップル社のiCloudサービスにデータをバックアップした途端、この保護は消えてしまう。
- アップル社の位置情報追跡（Find Myソフトウェアや AirTagsハードウェアを含む）は、令状に対して完全に脆弱である。

妊娠中の人々を保護するためには、Apple社はクラウドサービスの暗号化方法を完全に変更し、ユーザー、そしてユーザーのみが自分自身のデータの鍵を持つようにする必要がある。

ネット監視：：ハイテク産業 (Amazon)

アマゾンをはじめとする小売業者

購入データの保存、集計、共有方法を精査しなければならないだろう。

- このような企業は、すべての処方薬について厳格な記録保持要件を課せられているが、FDA がこの中絶薬を市販薬とするよう世論の圧力に屈した場合、ミフェプリストン (経口中絶薬) の販売データについて、より大きな自由裁量を得る可能性がある。
- オンライン小売業者は、妊娠を中断させるために (FDA の承認なしに) 添付文書外で使用することができる他の薬やサプリメントの販売情報を精査される可能性が高い。
- 中絶反対の州は、中絶薬に関するインターネットの取り締まりを強化するにつれて、中絶を望む人たちは、よりリスクの大きな医薬品やサプリメントへの依存を増やすことになる。

ネット監視：ハイテク産業 (健康アプリ)

健康データアプリ、特に生理日トラッカー

警察にとって有力なデータ源である。生理日トラッカーは何百万人ものアメリカ人にとって不可欠なツールだが、今や政府の監視役にもなりつつある。完璧なアプリは存在しないが、プライバシー保護アプリは将来、より大きな安全性を提供することができる。ユーザーの端末にローカルにデータを保存したり、遠隔地に保存されたデータにユーザーだけがアクセスできるようにすることで、セキュリティを向上させることができる。クラウドデータにエンドツーエンドの暗号化を使用し、アプリプロバイダーがパスワードをリセットしたり、暗号化キーをバイパスしたりできないようにすることで、会社は裁判所命令に従う能力を制限することができる。プロバイダーは、集計された「匿名」ユーザーデータの収集を一切行わず、アプリが機能するために必要な最小期間のみユーザーデータを保持することで、ユーザーをさらに保護することができる。ベストプラクティスとして、健康アプリは、アプリが政府の監視対象であるかどうかを通知する、いわゆる「令状フラグ」をインストールすることができる。

ネット監視：携帯電話、電子マネー決済

- 携帯電話は現代生活のいたるところにあるものだが、同時に、追跡のためのネットワークも提供している。携帯サイトの位置情報、GPS、ブルートゥースやWi-Fiネットワークの近接データ、その他数え切れないほどのデータポイントの間で、携帯電話を使用しているときに自分の位置を完全に隠すことは不可能だ。使い捨ての携帯電話は、位置情報の追跡からより大きな保護を提供することができるが、安全に購入し使用しない限り、簡単にユーザーとつながることができる。
- ほとんどすべての電子決済は、法執行機関によって容易に追跡され、識別される。数十年にわたる反マネーロンダリング・インフラストラクチャのおかげで、現金以外のほぼすべての形態の支払いについて、広大な監視インフラストラクチャが構築されている。警察はますます大量の暗号通貨取引を追跡できるようになり、数年後でも当事者を特定できるようになっている。しかし、金融機関は1万ドルを超える金融取引をレポートすることが義務付けられており、1万ドルの報告基準を意図的に回避して支払いを構成することは連邦犯罪である。

対抗手段：法、制度的な対応

対抗手段の提案

- 警察の法執行権限の制限
  - 警察が偽のアカウントを作成することを禁じる
  - ソーシャルメディアのアカウント情報を提供するよう強要することも禁止
  - 情報共有協定、情報融合センター、省庁間タスクフォース、連邦および州外の法執行機関とのその他のパートナーシップから脱退することで、管轄区域内の妊娠中の人々に対する監視の脅威を劇的に軽減。非正規滞在者を対象とした情報共有を制限するという現在進行中の要求にも応える
- 州は民間のデータブローカーがリプロダクティブ・ヘルスに関する情報を売買することを禁止する措置をとること

警察は裁判所の命令が得られない場合、データブローカーから簡単に情報を購入することができる。

- 2023年6月「私の身体、私のデータ」法案(Sara Jacobs議員)。リプロダクティブ・ヘルス情報の自己、自己コントロールの権利。多くのインターネットのプライバシーや人権団体が支持を表明。 (EFF)私の身体、私のデータ」法を支持する https://cryptpad.fr/pad/#/2/pad/view/yN6OLfK2ruywEmfTeC+Wd3poL8p0OxhmrbpvXjMxJY8/

対抗手段：暗号化、プライバシー・バイ・デザイン

対抗手段の提案

- 暗号化やその他の安全策によって電子記録を隠す。技術的なセーフガードは妊娠中の人々や彼らを支援する人々を強力に保護することができる

※有力な生殖医療提供者である家族計画連盟：そのウェブサイトに70近い広告トラッカーとサードパーティ・クッキーを設置しており、訪問者の身元を多数の広告ブローカーに明らかにしていることが判明

参考：「(MarkUp)非営利団体のウェブサイトは広告トラッカーだらけだ」https://themarkup.org/blacklight/2021/10/21/nonprofit-websites-are-riddled-with-ad-trackers
（仮訳）https://cryptpad.fr/pad/#/2/pad/view/KMGlAifAMomVx08IJoxkT58jWPElO3lf4MqZTCLgXtA/

- プロバイダーは、プライバシー・バイ・デザインの原則をデジタルプラットフォームに導入し、サービスに絶対に必要なデータだけを収集し、必要な期間だけ保持し、第三者による共有を最小限に抑えることで、自分自身と患者を守ることができる。
- 中絶医療提供者やその他の機関は、第三者のソーシャルメディアやメッセージングサービスの使用を含め、すべての電子的コミュニケーションのプライバシー監査を直ちに実施すべき

対抗手段： VPN

追跡がもたらす脅威を完全に排除することは不可能だが、脅威のモデル化によって、個人はプライバシーを守るために優先すべき手順を特定することができる。個人は、最大のプライバシーリスクを生み出す項目をリストアップすることから始め、最も簡単な解決策が利用可能なものに優先順位をつけ、より深刻で解決が困難なリスクへとリストを機能させていくことができる。

ウェブブラウジングは、常に政府と民間による広範な追跡の対象となる。

妊娠中の人々は、仮想プライベート・ネットワーク（ VPN ）を利用する

- 喫茶店や空港、場合によっては自宅など、安全でない共有ネットワークを使用する場合に特に重要である（自宅のネットワークが、ユーザーが監視されることを恐れている誰かによって管理されている場合）。
- VPN はまた、ユーザーのインターネット・プロトコル（ IP ）アドレスをウェブサイトやサービスから隠蔽し、ユーザーの位置情報も見えなくする。しかし、サイトは、クッキー、広告トラッカー、ブラウザのフィンガープリントなど、ユーザーを特定するために他のさまざまな方法を使用することができる。さらに、 VPN を使用する場合、インターネットの活動は VPN オペレータに見えるままであり、中にはユーザーデータを商業化したり、法執行機関に協力したりするものもある。

対抗手段： TOR 、エンド・ツー・エンド暗号化

- The Onion Reuter (TOR) ネットワークを使用することで、プライバシーの保護を得ることができる。単一のサーバーを経由してインターネット活動をルーティングする VPN とは異なり、 TOR は一連の 3 つの中継サーバーを経由してコンテンツをルーティングする。このアプローチにより、ユーザーの IP アドレスは、通信先のサービスからも、その間のサーバーからも隠蔽される。
- VPN 、 TOR 、またはその 2 つを組み合わせて使用することで、第三者のトラッキングを減らすことができるが、どのツールもユーザーに完全な匿名性を付与することはできず、法執行機関はこれらのテクノロジーを危険にさらすことで積極的に活動している。
- エンドツーエンド暗号化されたメッセージングツールを使用。の記事の発表時点では、 Signal が最も強固なセキュリティを提供している。それでも、メッセージがデバイスに保持されていれば、真に安全とは言えない。メッセージの自動削除／消滅を有効にすることで、ユーザーは、自分または相手のデバイスが後に危険にさらされた場合、暴露されるデータ量を減らすことができる。

まとめ

冒頭でマイナ保険証の問題に言及した。現在米国で起きている中絶犯罪化の急速な広がりと、これに対する抵抗の闘いをみたとき、

- 民主主義の手続を経て法が人権を蹂躙する力をもつことがある。
- 「法」が監視技術を正当化し、監視技術は更に法の隙間を衝いて開発される。

しかし

- 「悪法」を覆す可能性は常にある。
- 監視技術を阻む技術の可能性は常にある。

「監視技術を阻む技術」とはどのような技術なのかを知らなければ、対抗できない。

まとめ

- 番号を媒介にして私の医療情報が、治療や診療行為とは無関係に拡散する仕組みへの危機感をもつ必要がある。ジェイコブ議員が提出した「私の身体、私のデータ法」のように「個人の生殖または性に関する健康情報を収集、保持、使用、または開示」を厳しく制限する主張は、番号と医療情報の紐付けを禁止することになる。こうした原則的な法を提起することには意味がある。
- しかし「法」の限界は明らか。法がどのようであれ、私たちの人権を防衛するための手段を持つ必要がある。ネットの情報通信が支配的な現状において、重要な手段になるのは、匿名化と暗号だ。
- 中絶、ジェンダーを肯定するためのだけでなく、医療の対象となる分野は、不当な差別や偏見にさらされやすいことを念頭に、医療情報の原則をたてることが必要である。このことは差別や偏見と闘い人々の文化や価値観を変えることが、困難だが重要な課題になることを示している。

参考資料

- (fastcompany.com)MTA の OMNY マシンへの切り替えはプライバシーの悪夢である https://cryptpad.fr/pad/#/2/pad/view/n1I3keoQ62A2CdQqYdB-p6DexlhR453bnDLDC6+qM8w/
- (hasbrouck.org) 乗客名記録（PNR）には何が書かれているのか？ https://cryptpad.fr/pad/#/2/pad/view/Yi6PJ9Dl5wUzenfDwmF5z5g-yTeq1dTH0HCNaxD7c-g/
- (EFF) 自動ナンバープレート・リーダー（ALPR） https://cryptpad.fr/pad/#/2/pad/view/Q5549gZP2RfpmmRHoUzL5ShkYzq2eE2vroMYe0VhBxY/
- (MArkUp) 非営利団体のウェブサイトは広告トラッカーだらけだ https://cryptpad.fr/pad/#/2/pad/view/KMGlAifAMomVx08IJoxkT58jWPElO3lf4MqZTCLgXtA/
- 中絶禁止から 6 カ月、米国の 24 州が中絶を禁止、あるいは禁止する可能性がある： ラウンドアップ https://cryptpad.fr/pad/#/2/pad/view/fAv3w4Gc8dQPt+nAjdIURruatOMn59KT3xbWNF4gVcg/
- (EFF) 「私の身体、私のデータ」法を支持する https://cryptpad.fr/pad/#/2/pad/view/yN6OLfK2ruywEmfTeC+Wd3poL8p0OxhmrbpvXjMxJY8/

プライバシーツールと関連情報

- アクセスしたウエッブにどれだけのトラッカーが組込まれているのかを調べる。(Blacklight) https://themarkup.org/blacklight
- マジックミラーの裏側で：企業監視テクノロジーの詳細
  https://www.jca.apc.org/jca-net/sites/default/files/2022-10/eff_report_201912_print.pdf
- 反対派を防衛する─社会運動のデジタル弾圧と暗号による防御
  https://www.jca.apc.org/jca-net/sites/default/files/2021-11/%E5%8F%8D%E5%AF%BE%E6%B4%BE%E3%82%92%E9%98%B2%E8%A1%9B%E3%81%99%E3%82%8B(%E7%B5%B1%E5%90%88%E7%89%88).pdf
- 反監視運動情報
  https://www.alt-movements.org/no_more_capitalism/hankanshi-info/

ありがとうございます